CLAIMS:

1. A method of automatically obtaining a second certificate for a user using a first certificate, the method comprising:

accessing a registration server using a user's server and the first certificate of the user to create a connection that authenticates both the user's server identity via a server certificate of the user server and the user's identity via the user's first certificate;

creating a secure data channel between the registration server and the user server;

forwarding a request for the second certificate from the user server to the registration server;

determining in the registration server that the user is entitled to the second certificate;

forwarding a request from the registration server to an authority to generate a private/public key pair;

sending the private key to the user from the authority via the secure data channel;

sending the public key from the authority to another authority to be signed; and

forwarding the second certificate from the another authority to a directory.

2. The method of claim 1, further comprising sending a backup copy of the private key from the authority to a key recovery authority.

3. The method of claim 1, wherein the first certificate comprises a signature certificate.

4. The method of claim 1, wherein the second certificate comprises an encryption certificate.

5. The method of claim 1, wherein the first certificate comprises an expiring signature certificate and the second certificate comprises a replacement signature certificate.

6. The method of claim 1, wherein the first certificate comprises a signature certificate and the second certificate comprises a replacement encryption certificate.

7. The method of claim 1, wherein the first certificate comprises a signature certificate and the second certificate comprises one of either the user's current encryption certificate or an expired encryption certificate of the user.

8. A method of automatically obtaining a second certificate for a user using a first certificate, the method comprising:

accessing a server platform using a user's server and the first certificate of the user to create a connection that authenticates both the user's server identity via a server certificate of the user server and the user's identity via the user's first certificate;

creating a secure data channel between the server platform and the user server;

forwarding a request for the second certificate from the user server to the server platform; and

generating at the server platform the second certificate.

9. The method of claim 8, wherein the first certificate comprises a signature certificate.

10. The method of claim 8, wherein the second certificate comprises an encryption certificate.

11. The method of claim 8, wherein the first certificate comprises an expiring signature certificate and the second certificate comprises a replacement signature certificate.

12 14. The method of claim 8, wherein the first certificate comprises a signature certificate and the second certificate comprises a replacement encryption certificate.

13 15. The method of claim 8, wherein the first certificate comprises a signature certificate and the second certificate comprises one of either the user's current encryption certificate or an expired encryption certificate of the user.

Rule 1.126 Deficiency Notice

14 16. An apparatus for automatically obtaining a second certificate for a user using a first certificate, the apparatus comprising:

a user server and a registration server, the user server accessing the registration server using the first certificate of the user to create a connection that authenticates both the user's server identity via a server certificate of the user server and the user's identity via the user's first certificate;

a secure data channel, the secure data channel being disposed between the registration server and the user server, the user server forwarding a request for the second certificate to the registration server through the secure data channel;

a first authority, the registration server determining that the user is entitled to the second

certificate and forwarding a request to the first authority to generate a private/public key pair, the first authority sending the private key to the user via the secure data channel;

a second authority, the first authority sending the public key to the second authority to be signed; and

a directory, the second authority forwarding the second certificate to the directory.

17. The apparatus of claim 14, wherein the first certificate comprises a signature certificate.

18. The apparatus of claim 14, wherein the second certificate comprises an encryption certificate.

19. The apparatus of claim 14, wherein the first certificate comprises an expiring signature certificate and the second certificate comprises a replacement signature certificate.

20. The apparatus of claim 14, wherein the first certificate comprises a signature certificate and the second certificate comprises a replacement encryption certificate.

~~21~~ 19. The apparatus of claim ~~16~~ 14, wherein the first certificate comprises a signature certificate and the second certificate comprises one of the user's current encryption certificate and an expired encryption certificate of the user.

~~22~~ 20. An apparatus for automatically obtaining a second certificate for a user using a first certificate, the apparatus comprising:

a user server and a server platform, the user server accessing the server platform using the first certificate of the user to create a connection that authenticates both the user's server identity via a server certificate of the user server and the user's identity via the user's first certificate;

a secure data channel, the secure data channel being disposed between the server platform and the user server;

the user server forwarding a request for the second certificate to the server platform; and

the server platform generating the second certificate.

~~23~~ 21. The apparatus of claim ~~22~~ 20, wherein the first certificate comprises a signature certificate.

24. The apparatus of claim 20, wherein the second certificate comprises an encryption certificate.

25. The apparatus of claim 20, wherein the first certificate comprises an expiring signature certificate and the second certificate comprises a replacement signature certificate.

26. The apparatus of claim 20, wherein the first certificate comprises a signature certificate and the second certificate comprises a replacement encryption certificate.

27. The apparatus of claim 20, wherein the first certificate comprises a signature certificate and the second certificate comprises one of either the user's current encryption certificate or an expired encryption certificate of the user.